ON PAGE 37   10 June 1985

Spying Through Computers?

The Defense Department's computer system is vulnerable.

The scenario has become a classic: a teen-age computer hacker breaks into the NORAD computer system and starts a countdown to World War III. Robert Brotzman, director of the Department of Defense Computer Security Center at Fort Meade, is often asked whether that scene from the movie "WarGames" could really happen—and he generally replies cautiously that it's not altogether impossible. But that may be something of an understatement. A recent study by his own office—the first such study ever—determined that only 30 out of about 17,000 DOD computers surveyed meet minimum standards for protection. Brotzman's reluctant conclusion: "We don't have anything that isn't vulnerable to attack from a retarded 16-year-old." And although no major spy case—including the Navy scandal—has yet involved computers, Brotzman's findings suggest that the high-tech world poses a new potential threat to the nation's security.

Gone are the days when all secret materials were consigned to lead-lined filing cabinets and vaults conspicuously marked "CLASSIFIED" and only those with proper clearances were able to gain access. The computer age has changed all that, and DOD computers handle virtually everything from targeting ICBM's to parceling out spaces in the Pentagon parking lot. But the secrets inside those electronic filing cabinets aren't nearly as well guarded as paper documents. "If we treated our beer like we treat our information," says Brotzman, "we'd all be dead from bad booze."

Rules: Brotzman's team sought to ascertain whether the DOD computers were capable of self-policing: could the computers themselves essentially perform the function of a soldier standing guard over the filing cabinets? For 99.9 percent of the computers, the answer was no—for reasons ranging from bad password controls (the problem in "WarGames") to poorly enforced rules on who can read, write and copy classified information. About 60 percent of the systems surveyed can be upgraded at minor cost, some simply by changing the operating system. But the rest pose far tougher problems, including age and obsolescence. As disturbing as the findings were, the situation may actually be even worse. Brotzman learned that the U.S. government doesn't even know how many computers the Defense Department uses. In addition, more than two-thirds of the DOD offices, including some of its most sensitive outposts, failed to return the survey forms.
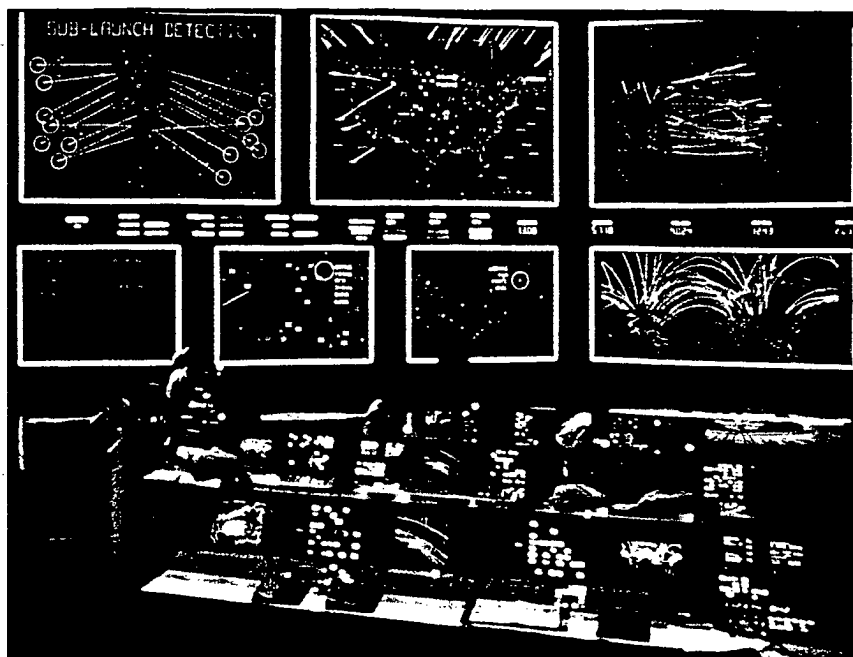
The incredible speed and seemingly infinite capacity of modern computers tend to make them more difficult to control. That difficulty has been compounded by the problems of convincing computer-illiterates, awed by the dazzling new technologies, that the new systems are vulnerable in a wide variety of ways. For example, computer chips retain data even after it is cleared from a screen. So do discs and tapes, unless they are painstakingly erased. And while the threat of random-dialing KGB agents—or teen-agers—has been virtually eliminated by a well-enforced policy that links computers containing classified information only to special, secure phone lines, much vital military information remains unclassified. One prime example is the military's computerized supply system, which is accessible from almost any phone, thus giving skilled hackers the opportunity to manipulate supplies of critical items like spare parts or fuel.

Moreover, the computer is open to a broad range of high-tech hit-and-run spying techniques. A clever technician could rig up a "Trojan horse" program that might allow an unauthorized user access to a system. Or a spy might implant what are called "spoof" programs, which feign normal activity while busily collecting passwords or other useful information. The most frightening prospect of all is so-called computer "viruses"—undetectable instructions, which can be hidden deep inside software, to destroy or alter data.

In the wake of its survey—ordered under a new presidential policy on information security issued last September—the DOD Computer Security Center has invited industry to develop new systems that meet its security standards. But so far just one product qualifies for the highest classification of secret information—and that product isn't compatible with most government computers. In fact, only three other products can be used at all. Single-microprocessor computers like the IBM PC, where the security system is built into the software, don't qualify for classified use because a sophisticated user could tinker with the software.

Genius: Despite the surfeit of spy scandals in recent years, none so far has involved the nation's computer systems. And as long as computer espionage remains the province of screenwriters, many will continue to suspect that Brotzman is exaggerating the potential danger. Indeed, some argue that the current Navy spy scandal reinforces the notion that the real danger lies elsewhere. "They're putting their defenses in the wrong places," insists computer-security expert Robert Courtney Jr. "They're trying to protect against the technical genius rather than the low-level clerk."

But Brotzman thinks otherwise. The techniques of today's computer thieves are too sophisticated (no fingerprints, even electronic ones), and the targets are too inviting (a single computer disc equals hundreds of paper pages) to ignore, as he sees it. "Considering how much fun the bad guys could have on U.S. computers," says Brotzman, "if they ain't having at them, they're a lot dumber than we think they are."

RICHARD SANDZA at Fort Meade, Md.

Scene from the movie 'WarGames': Could it actually happen to the Department of Defense?